PRE-APPEAL BRIEF REQUEST FOR REVIEW	Docket Number (Optional) 014801-000400US

I hereby certify that this correspondence is being filed via EFS-Web or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)] on May 16, 2008 Signature / Stephanie Klepp / Typed or printed name Stephanie Klepp	Application Number 09/360,068	Filed July 23, 1999
	First Named Inventor Kevin J. Page	
	Art Unit 2135	Examiner Paula W. Klimach

Applicants request review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

□ applicant/inventor.

□ assignee of record of the entire interest.
See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)

☒ attorney or agent of record.
Registration number 55,127.

□ attorney or agent acting under 37 CFR 1.34.

Registration number if acting under 37 CFR 1.34. ________

Signature

Michael L. Drapkin
Typed or printed name

303.571.4000
Telephone number

May 16, 2008
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☒ *Total of 1 forms are submitted.

I hereby certify that this correspondence is being filed via
EFS-Web with the United States Patent and Trademark Office
on May 16, 2008.

TOWNSEND and TOWNSEND and CREW LLP

By: / Stephanie Klepp /
Stephanie Klepp

PATENT
Attorney Docket No.: 014801-000400US
Client Ref. No.: PD482

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Kevin J. Page, et al.

Application No.: 09/360,068

Filed: July 23, 1999

For: METHOD AND APPARATUS FOR ESTABLISHING A SECURE SMART CARD COMMUNICATION LINK THROUGH A COMMUNICATION NETWORK

Customer No.: 20350

Confirmation No. 3638

Examiner: Paula W. Klimach

Technology Center/Art Unit: 2135

ARGUMENTS FOR PRE-APPEAL BRIEF REQUEST FOR REVIEW

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

This statement constitutes the Arguments in support of the Pre-Appeal Brief Request for Review, which is submitted herewith along with a Notice of Appeal. Applicants respectfully request review and withdrawal of the Final Office Action ("Office Action") mailed February 20, 2008.

The Office Action maintained rejection of claims 1, 2, 4-18, 20-27, 29-35, and 59 under 35 U.S.C. §103(a) as being unpatentable over various combinations of the cited portions of U.S. Patent No. 6,101,477 to Hohle et al. ("Hohle"), U.S. Patent No. 5,414,772 to Naccache ("Naccache"), U.S. Patent No. 6,304,223 to Hilton et al. ("Hilton"), and U.S. Patent No. 6,226,744 to Murphy et al. ("Murphy"). The cited references cannot be relied upon to teach or suggest the limitations of independent claims 1, 17, 18, 21, 22, 25, or 29 and, therefore, Applicants believe all claims now pending are allowable.

These independent claims each include limitations relating to an outgoing secure communications link from a **smart card**, through a **smart card communication device**, and to a **remote central computer system**.

The cited references do not teach or suggest:

1) Secured data formatted ***by the smart card*** to allow the ***central computer system*** to ***detect a modification*** to the secured data occurring during transmission beginning at the smart card, passing through a smart card communication device, and extending through to the remotely located central computer system, as generally recited in claims 1, 17, 21, 22 or 29; or

2) A second set of secured data, the second set formatted ***by the central computer system*** to allow the ***smart card*** to ***detect a modification*** to the second set occurring during transmission *beginning at the remote central computer system*, passing through a smart card communication device, and *extending to the smart card*, as recited in claim 17, 18, and 25; or

3) the smart card communications device "transmitting the outgoing" signal to a *remote* central computer system "without deciphering the data," as set forth in claim 1 or 23;

1) + 2) Detection of a Modification to the Secured Data beginning at the Smart Card and Extending to the the Central Computer System

The identified claims set forth a secure communication link *between* a ***smart card***, *through a smart card communication device* remote , and to a ***central computer system***. In some claims, the central computer detects modification to the secured data beginning at the smart card and extending through to the central computer. In other embodiments, the smart card detects a modification in the reverse direction, beginning at the central computer and extending through to the smart card. Again, it is worth noting that the central computer system is located remotely from the smart card and the smart card communication device.

Naccache does not appear to be cited for these limitations, as the Office Action appears to rely on Hohle to teach the missing elements (Office Action, p. 4, ll. 19 - p. 5, l. 2; p. 10, ll. 14-17, both *citing* Hohle, col. 22, ll. 47-67). The Office Action indicates that it is the issuer 10 of Hohle that reads on the central computer system of the claims (Office Action, p. 4, ll. 8-16, *citing* Hohle Fig. 10).

However, the cited passages of Hohle address "'signing' of the data using a message authentication code" for transmission between the card and the **external device** (emphasis added, Hohle, col. 22, ll. 50-57). Hohle describes the "external device" to be "a **card reader,**" and communication to the external device is through "a line for serial data communication" (Hohle, col. 3, ll. 3-4, 24-25, emphasis added). Serial data communication between a smart card and a card reader falls far short of the secure communication from a smart card to a remote central computer system. Hence, Hohle also falls short of the limitation relating to end-to-end data integrity *from* a smart card, *passing through* a smart card communication device, and extending to a *remote* central computer system.

Moreover, it is worth noting that the Specification describes a rationale for certain aspects of such embodiments, noting that "that security devices at the central computer system may be replaced or exchanged without affecting the smart card communication device. ... [Such embodiments provide for methods of] establishing a secure communication link between a smart card and a central computer system through a communication network by allowing data to transparently pass through a smart card communication device, processor and communication network and by performing security functions at the smart card and the central computer system." (Original Application, p. 4, l. 26 - p. 5, l. 19)

3) Secured Data Received and Transmitted by a Smart Card Communication Device to a Remote Central Computer

The Office also concedes that "Hohle does not expressly disclose the outgoing transmission sent [from the smart card communication device] without deciphering the data" (Office Action, p. 5, ll. 3-5). Additionally, the Office Action concedes that "Hohle does not teach receiving at a smart card communication device an outgoing message and using the smart card communication device to produce an outgoing secure data signal" (Office Action, p. 5, ll. 5-7). Thus, the Office concedes that much of the functionality (steps for receiving, demodulating, and producing an outbound signal) for the outbound communication that occurs at the smart card communication device is absent from Hohle

The Office Action appears to rely on Naccache to teach the missing elements. However, Applicants respectfully submit that the Office Action has erred in this reliance.

Claim 1 recites that the "outgoing ... signal transmitted from the smart card" is "demodulat[ed] using the smart card communication device [to] produce an outgoing secure data signal . . . without deciphering the secured data, and is then transmitted to a central computer system "remote from the smart card communication device."

Naccache, in contrast, describes communication between a "chip card" and "a computer . . . comprising a chip reader enabling **physical communication** with the card," through an "**I/O interface**" (emphasis added, Naccache, col. 3, ll. 33-45; Fig. 3). In Naccache, the communication described is only between the "chip card" and the "chip reader" via the "interface." (Naccache, col. 3, ll. 32-45). Therefore, the Office's reliance on Naccache to teach communication between a smart card communication device and a remote central computer system is misplaced (Office Action, p. 5, ll. 11-16, *citing* Naccache, col. 6, ll. 1-11).

The Office improperly relies on Naccache to teach certain outgoing communication methods and signals that, in certain claims, are processed at the smart card communication device and then transmitted to the remote central computer system. For example, the Office Action states that apparatus B of Naccache "corresponds to the central computer system." (Office action, p. 5, ll. 15-16). This assertion is in error, as the chip reader (Apparatus B) is a local computer in physical communication with a chip card. Communication from a smart card to a *local* reader fails to teach the communication from a smart card through a smart card communication device through to a *remote* central computer system, recited in certain claims.

The Office improperly relies on Naccache to teach "using the smart card communication device to produce an outgoing secure data signal" destined for a remote central computer system (Office Action, p. 5, ll. 11-14, *citing* Naccache, col. 2, ll. 56-58). The cited portions of Naccache are from a smart card to the reader, and very clearly fall short of teaching the limitations of the claims related to communications with a remote central computer system.

CONCLUSION

For at least these reasons, it is respectfully submitted that independent claims 1, 17, 18, 21, 22, 25, and 29 are allowable. Claims 2, 4-16, 20, 23-24, 26-27, 30-35, and 59 each depend from the independent claims, and these claims are believed to be allowable for at least the same reasons. Applicants respectfully request that the rejection be withdrawn. Applicants believe all pending claims are allowable over their cited references, and thus request the issuance of a Notice of Allowance at an early date.

Respectfully submitted,

Michael L. Drapkin
Registration No. 55,127

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 303-571-4000
Fax: 415-576-0300

MLD/sk
61352585 v1